Euclidean domain, PID, UFD

PID Principal Ideal Domain

UFD Unique Factorization Domain

Euclidean Domain

Let R be an integral domain.

Defn: (Division) Let $a, b \in R$, $a \neq 0$. We say that a divides b denoted as $a|b$ if $b = aq$ for some $q \in R$.

EUCLIDEAN DOMAIN Defn:

An Euclidean domain is an integral domain R with a map

$$\text{Norm} : R - \{0\} \longrightarrow \mathbb{N}$$ such that

1) For $a, b \in R$ if $a|b$ then

$$\text{Norm}(a) \leq \text{Norm}(b).$$

2) For any $a, b \in R$ with $b \neq 0$

there exist $q, r \in R$ such that

$a = bq + r$ and either

$r = 0$ or

$\text{Norm}(r) < \text{Norm}(b)$.

Examples: 1) $\mathbb{Z}$ $\quad \text{Norm}(n) = |n|$

2) F field, $F[x]$ $\quad \text{Norm}(f) = \deg(f)$

3) Gaussian integers

$$\mathbb{Z}[i] = \{ a+bi \mid a, b \in \mathbb{Z} \}$$

→ $\mathbb{Z}[i]$ is a commutative ring.

→ $\mathbb{Z}[i]$ is an integral domain.

$$\text{Norm} : \mathbb{Z}[i] - \{0\} \longrightarrow \mathbb{N}$$

$$a+bi \longmapsto a^2+b^2$$

→ $\mathbb{Z}[i]$ is an Euclidean domain.

Suppose $\alpha \mid \beta$, $\beta = \alpha\gamma$

$$\text{Norm}(\beta) = \text{Norm}(\alpha\gamma)$$
$$= \text{Norm}(\alpha)\,\text{Norm}(\gamma)$$

$\Rightarrow \text{Norm}(\alpha) \leq \text{Norm}(\beta)$.

→ Suppose $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$.

$\alpha = a+bi$ $\qquad N(\beta) \leq N(\alpha)$

$\beta = c+di$

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{a+bi}{c+di}\,\frac{(c-di)}{(c-di)}$$

(think in $\mathbb{C}$)

$$= \frac{(ac+bd)+(bc-ad)i}{c^2+d^2}$$

Let m be the closest integer to $\frac{ac+bd}{c^2+d^2}$ but smaller than $\frac{ac+bd}{c^2+d^2}$

Let n be the $\frac{bc-ad}{c^2+d^2}$

Define $q = m+ni$ $\quad \text{Norm}\left(\frac{\alpha}{\beta} - q\right) \leq \frac{1}{2}$

and $r = \alpha - \beta q$

$$r = \beta\left(\frac{\alpha}{\beta} - q\right)$$

$$\text{Norm}(r) = \text{Norm}(\beta)\ \text{Norm}\left(\frac{\alpha}{\beta} - q\right)$$

$$\leq \frac{\text{Norm}(\beta)}{2} < \text{Norm}(\beta)$$

So, r & q are remainder & quotient respectively.

4) Eisenstein Integers

$$\mathbb{Z}[w] = \{a+bw) \quad a,b \in \mathbb{Z}\}$$

$$\text{Norm}(a+bw) = a^2+b^2-ab \quad \text{---} *$$

Exc: $\mathbb{Z}[w]$ is an Euclidean domain with respect to norm defined by $*$.

Principal Ideal Domain

Defn (PID) Let R be an integral domain. We say that R is a PID if every ideal of R is principal, i.e., if $I \subseteq R$ an ideal, then $I = \langle a \rangle$ for some $a \in R$.

$$\langle a \rangle = \{ar \mid r \in R\}$$

Examples: $\mathbb{Z}$, $F[x]$ (where F is a field)

Thm: If R is an Euclidean domain, R is a PID.

Pf: Let I be an ideal of R.

If $I = \{0\}$, then $a = 0$ is one generator for I.

Otherwise, choose some $a \in I$, $a \neq 0$ such $N(a)$ is smallest among all norms

of elements in I.

If $\beta \in I$, then $N(\beta) \geq N(a)$.

Since R is an Euclidean domain, there exists q and r such that

$$\beta = aq + r$$

Since $\beta \in I$, $aq \in I$, $r = \beta - aq \in I$

So, r cannot be non-zero because that would imply that $\text{Norm}(r) < \text{Norm}(a)$, a contradiction.

Hence $r = 0$.

$$\text{So, } I = \langle a \rangle.$$

- Converse is false.

Consider $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{ a + b\left(\frac{1+\sqrt{-19}}{2}\right) \middle| \begin{matrix} a,b \\ \in \mathbb{Z} \end{matrix} \right\}$

$\downarrow$

PID but not Euclidean domain.

Primes and Irreducibles

Defn (Prime) Let R be an integral domain. An element $a \in R$ is called **prime** if:

a) $a \neq 0$ and a is not invertible in R.

b) If $a \mid bc$ for $b, c \in R$ then either $a \mid b$ or $b \mid c$.

Defn: (Irreducible) Let R be an integral domain. We say that $a \in R$ is an **irreducible** if:

a) $a \neq 0$ and a is not invertible in R.

b) If $a = bc$ then either b or c is invertible in R.

Lemma: If a is prime, then a is irreducible.

Pf: Assume a is prime.

Suppose $a = bc \Rightarrow a \mid bc \Rightarrow a \mid b$ or $a \mid c$

If $a|b \Rightarrow b = aa' \Rightarrow bc = aa'c$

$\Downarrow$

$a = aa'c$

Since R is an integral domain

If $a = aa'c \Rightarrow a = 0$ or $a'c = 1$

$\downarrow$ not possible

$\downarrow$

c is invertible

Similarly if $a|c$ then b is invertible.

So, a is irreducible.

—

Converse is not true in general.

Consider $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

We have a norm function on $\mathbb{Z}[\sqrt{-5}]$

Norm: $\mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{N}$

$a + b\sqrt{-5} \longmapsto a^2 + 5b^2$

Suppose $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is invertible

So $\alpha\beta = 1$

$$\text{Norm}(\alpha\beta) = \text{Norm}(1) = 1$$

$$\text{Norm}(\alpha)\,\text{Norm}(\beta) = 1$$

$$\Rightarrow \text{Norm}(\alpha) = 1$$

And conversely if $\text{Norm}(\alpha) = 1$, say $\alpha = a + b\sqrt{-5}$

$$\Rightarrow (a+b\sqrt{-5})(a-b\sqrt{-5}) = 1$$

So, α is invertible.

$$\text{Norm}(a+b\sqrt{-5}) = 1 \iff a^2 + 5b^2 = 1$$

$$\Updownarrow$$

$$a = \pm 1,\ b = 0$$

So the only elements in $\mathbb{Z}[\sqrt{-5}]$ that are invertible are ± 1.

Consider $2 \in \mathbb{Z}[\sqrt{-5}]$, 2 is irreducible because

i) $2 \neq 0$ and 2 is not invertible.

ii) If $2 = bc$, then

$$\text{Norm}(2) = \text{Norm}(b)\ \text{Norm}(c)$$

$$4 = \text{Norm}(b)\ \text{Norm}(c)$$

So, possibilities for Norm (b) are 1, 4 & 2.

If Norm $(b) = 1 \Rightarrow b$ is invertible

If Norm $(b) = 4 \Rightarrow$ Norm $(c) = 1 \Rightarrow c$ is invertible

If Norm $(b) = 2$, say $b = r + s\sqrt{-5}$

$\Rightarrow r^2 + 5s^2 = 2$, no solutions in $\mathbb{Z}$.

So 2 is irreducible, but 2 is not prime because

$2 \mid (1+\sqrt{5})(1-\sqrt{-5})$ but 2 neither divides $1+\sqrt{5}$, nor it divides $1-\sqrt{-5}$.

There are certain types of rings where these two notions agree, i.e. α is prime

$\Leftrightarrow$

α is irreducible.

Unique Factorization Domains

Defn: An integral domain is called an UFD if every non zero, non-invertible element α can be written as product of irreducibles, uniquely (upto reordering and multiplication by invertible elements.)

Examples: 1) $\mathbb{Z}$ is a UFD

2) If R is a UFD, $R[x]$ is a UFD.

Lemma: Let R be a UFD. If a is irreducible, then a is a prime.

Pf: Suppose $a \mid bc$.

If b or c is zero then $a \mid b$ or $a \mid c$.

If b is invertible $\Rightarrow bb' = 1$

$\Rightarrow cbb' = c \Rightarrow a \mid c$

Similarly if c is invertible, $a \mid b$.

Let us assume that b & c are non-zero and non-invertible.

$$b = p_1^{q_1} \cdots p_r^{q_r} \qquad q_i \geq 0$$

$$c = p_1^{b_1} \cdots p_r^{b_r} \qquad b_i \geq 0$$

Since $a \mid bc \Rightarrow bc = aa'$

By uniqueness, a has to be one of the primes p_i, if $q_i > 0$ $a \mid b$ otherwise $a \mid c$.

$\{\text{Euclidean Domain}\} \subsetneq \{\text{PID}\}$

Thm: If R is a PID, R is a UFD.

Pf: For next algebra Course!

$$\left\{\begin{matrix}\text{Euclidean}\\ \text{Domain}\end{matrix}\right\} \subsetneq \{\text{PID}\} \subsetneq \{\text{UFD}\}$$

Example of a UFD which is not a PID.

Consider $R = \mathbb{Z}[x, y]$, R is a UFD.

Consider $I = \langle x, y \rangle$.

If I is principal, that means

$$\langle x, y \rangle = \langle h \rangle$$

$x = hh_1$ for some $h_1 \in \mathbb{Z}[x, y]$.

$\Rightarrow$ $h = \pm x$ and $h_1 = \pm 1$ or

$h = \pm 1$ and $h_1 = \pm x$

If $h = \pm x$ then $y \notin \langle h \rangle$ Contradiction

If $h = \pm 1$

$\Rightarrow \quad 1 = xf + gy$

↓

no constant coefficient

So Contradiction.

So $R = \mathbb{Z}[x, y]$ is not a PID.